PCT/IB04/050813

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03101718.9

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03101718.9
Demande no:

Anmeldetag:
Date of filing: 12.06.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Verfahren zum Abwehren von mittels differentieller Stromanalyse erfolgenden Angriffen

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR LI

BESCHREIBUNG

Verfahren zum Abwehren von mittels differentieller Stromanalyse erfolgenden Angriffen

Die vorliegende Erfindung betrifft ein Verfahren zum Abwehren mindestens eines Angriffs, das mittels differentieller Stromanalyse bei mindestens einem hyperelliptischen Kryptosystem, insbesondere bei mindestens einem hyperelliptischen Public-Key-Kryptosystem, erfolgt, das durch mindestens eine hyperelliptische Kurve beliebigen Geschlechts über einem endlichen Körper in einer ersten Gruppe gegeben ist, wobei die hyperelliptische Kurve durch mindestens einen Koeffizienten gegeben ist.

Obwohl bis vor kurzem elliptische Kryptosysteme (= Systeme auf Basis sogenannter e[lliptic]c[urve]c[ryptography]) für schneller als hyperelliptische Kryptosysteme (= Systeme auf Basis sogenannter h[yperelliptic]c[urve]c[ryptography]) gehalten wurden, wurde bereits in der Vergangenheit der Gebrauch von Jacobischen Varietäten hyperelliptischer Kurven über endlichen Körpern als Alternative zu elliptischen Kurven für die Kryptographie vorgeschlagen (vgl. Neal Koblitz, "A family of Jacobians suitable for discrete log cryptosystems", in S. Goldwasser (Hrsg.), "Advances in Cryptology - CRYPTO '88", Band 403 der "Lecture Notes in Computer Science", Seiten 94 bis 99, 21. bis 25. August 1988, Springer-Verlag, 1990; Neal Koblitz, "Hyperelliptic Cryptosystems", Journal of Cryptology 1 (1989), Seiten 139 bis 150).

Zwei jüngste Entwicklungen lassen nun jedoch die Einschätzung, dass ecc-Systeme schneller als hec-Systeme sind, als änderungsbedürftig erscheinen:

Im September 2002 hat Kim Nguyen (Philips Semiconductors) die Ergebnisse seiner Implementierung von Tanja Langes projektiven Formeln (vgl. Tanja Lange, "Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/147, 2002, http://eprint.iacr.org/) in Geschlecht zwei auf einem experimentellen Hardware-Simulator beim ECC 2002 "Workshop on elliptic curve cryptography" in Essen beschrieben. Die Resultate ließen die Konkurrenzfähigkeit von hec vermuten.

Kurz danach haben J. Pelzl, T. Wollinger, J. Guajardo und C. Paar sehr effiziente Formeln für K urven des Geschlechts drei bekannt gemacht (vgl. J. Pelzl, T. Wollinger, J. Guajardo, C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves", eingereicht), einschließlich einer drastischen Verbesserung der Zeiten für die Verdopplung in einem wichtigen Fall und einer Implementierung auf einem "embedded microprocessor" (ARM7).

Mit der effizienten Realisierung von hec-basierten Systemen in Hardware, insbesondere auf Chipkarten, stellt sich unmittelbar die Frage nach der Sicherheit von hec in bezug auf differentielle Stromanalyse (sogenannte D[ifferential]P[ower]A[nalysis]). Die differentielle Stromanalyse wurde von P. Kocher, von J. Jaffe und von B. Jun in zwei Arbeiten (vgl. P. Kocher, J. Jaffe und B. Jun, "Introduction to Differential Power Analysis and Related Attacks", http://www.cryptography.com/dpa/technical, 1998; P. Kocher, J. Jaffe und B. Jun, "Differential Power Analysis", Lecture Notes in Computer Science, Band 1666, Seiten 388 bis 397, Springer-Verlag, Berlin, Heidelberg, 1999) eingeführt und wird in den zitierten Arbeiten beschrieben.

Kurze Beschreibungen der differentiellen Stromanalyse finden sich auch

- in den Abschnitten 3.2 und 3.3 der Arbeit von M. Joye und von C. Tymen, "Protections against Differential Analysis for Elliptic Curve Cryptography - An Algebraic Approach" in C. K. Koc, D. Naccache und C. Paar (Hrsg.): CHES 2001, "Lecture Notes in Computer Science", Band 2162, Seiten 377 bis 390, Springer-Verlag, Berlin, Heidelberg, 2001 oder
- in Abschnitt 3 der Arbeit von J.-S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems" in C. K. Koc und C. Paar (Hrsg.): CHES'99, "Lecture Notes in Computer Science", Band 1717, Seiten 292 bis 302, Springer-Verlag, Berlin, Heidelberg, 1999.

Solche DPA-Angriffe messen die Stromverbräuche kryptographischer Apparate während der Bearbeitung verschiedener Eingaben und setzen die Messungen in Korrelation mit den Werten von festgelegten Bits in der internen Darstellung der Daten. Die Idee der differentiellen Stromanalyse ist jedoch sehr allgemein und funktioniert auch mit weiteren physikalischen Größen, wie zum Beispiel mit elektromagnetischer Strahlung.

Die bisherigen Darstellungen zur Implementierung von hec-basierten Kryptosystemen waren hauptsächlich auf die Effizienz der Implementation fokussiert und vernachlässigten die Resistenz der Implementierung gegenüber Attacken mittels differentieller Stromanalyse.

Ausgehend von den vorstehend dargelegten Nachteilen und Unzulänglichkeiten sowie unter Würdigung des umrissenen Standes der Technik liegt der vorliegenden Erfindung die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art so weiterzubilden, dass ein wesentlicher Beitrag zu einer effizienten und sicheren Implementierung von Systemen auf Basis der hyperelliptischen Kryptographie geleistet werden kann.

Diese Aufgabe wird durch ein Verfahren mit den im Anspruch 1 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen und zweckmäßige Weiterbildungen der vorliegenden Erfindung sind in den Unteransprüchen gekennzeichnet.

Mithin basiert die vorliegende Erfindung auf dem Prinzip des Bereitstellens von Gegenmaßnahmen zum Abwehren von auf differentieller Stromanalyse beruhenden Angriffen auf Implementierungen hyperelliptischer Kryptosysteme, und zwar im speziellen darauf, dass die Skalarmultiplikation auf der Jacobischen Varietät einer hyperelliptischen Kurve durch Kurvenrandomisierung (im Sinne eines hyperelliptischen Analogons der Randomisierung von Kurven bei der vorstehend zitierten Arbeit von M. Joye und von C. Tymen) und/oder durch Divisorenrandomisierung (im Sinne eines hyperelliptischen Analogons der dritten Gegenmaßnahme der vorstehend zitierten Arbeit von J.-S. Coron: Randomisierung von Punkten - also hier Divisorenrandomisierung) gegen differentielle Stromanalyse resistent gemacht wird.

Auf diese Weise wird durch die beschriebene Erfindung ein wesentlicher Beitrag zur effizienten und sicheren Implementierung von h[yperelliptic]c[urve]c[ryptography]-basierten Systemen, das heißt in Richtung auf die Robustheit sowie Sicherheit von hec-basierten Kryptosystemen gegen derartige DPA-Angriffe geleistet, wobei neben den Techniken und der Ausführbarkeit nachfolgend auch die Komplexität derartiger Methoden betrachtet werden soll.

Die Grundidee bei der Kurvenrandomisierung besteht darin, die Bits von den Operanden unvorhersehbar zu modifizieren. Zu diesem Zwecke wird die gewünschte Berechnung nicht in der gegebenen Gruppe, sondern in einer zweiten, zufällig erzeugten, aber isomorphen Gruppe durchgeführt; sodann wird das Resultat in die erste Gruppe zurückgezogen.

Die Grundidee bei der Divisorenrandomisierung besteht darin, die Bits der Darstellung eines reduzierten Divisors, der üblicherweise das Basiselement des Kryptosystems ist, oder ein Zwischenergebnis der Skalarmultiplikation zu ändern. Die Technik der Divisorenrandomisierung kann eingesetzt werden, wann immer ein Gruppenelement auf mehrere unterschiedliche Weisen dargestellt werden kann.

Die vorliegende Erfindung betrifft des weiteren einen Mikroprozessor, arbeitend gemäß einem Verfahren gemäß der vorstehend dargelegten Art.

Die vorliegende Erfindung betrifft des weiteren eine Vorrichtung, insbesondere Chipkarte und/oder insbesondere Smart-Card, aufweisend mindestens einen Mikroprozessor gemäß der vorstehend dargelegten Art.

Die vorliegende Erfindung betrifft schließlich die Verwendung

- eines Verfahrens gemäß der vorstehend dargelegten Art und/oder
- mindestens eines Mikroprozessors gemäß der vorstehend dargelegten Art und/oder

- mindestens einer Vorrichtung, insbesondere mindestens einer Chipkarte und/oder insbesondere mindestens einer Smart-Card, gemäß der vorstehend dargelegten Art

beim Abwehren mindestens eines mittels differentieller Stromanalyse auf mindestens ein hyperelliptisches Kryptosystem, insbesondere auf mindestens ein hyperelliptisches Public-Key-Kryptosystem, erfolgenden Angriffs; hierbei bedient sich ein Public-Key-Kryptosystem üblicherweise eines asymmetrischen Verschlüsselungsverfahrens.

Wie bereits vorstehend erörtert, gibt es verschiedene Möglichkeiten, die Lehre der vorliegenden Erfindung in vorteilhafter Weise auszugestalten und weiterzubilden. Hierzu wird einerseits auf die dem Anspruch 1 nachgeordneten Ansprüche verwiesen, andererseits werden weitere Ausgestaltungen, Merkmale und Vorteile der vorliegenden Erfindung nachstehend unter anderem anhand der durch Figur 1 veranschaulichten exemplarischen Implementierung gemäß einem Ausführungsbeispiel näher erläutert.

Es zeigt:

Fig. 1 in schematischer Darstellung ein Ausführungsbeispiel für ein auf dem Prinzip der Kurvenrandomisierung beruhenden Verfahren gemäß der vorliegenden Erfindung.

Bevor nachstehend anhand eines ersten Ausführungsbeispiels die Methode der Kurvenrandomisierung veranschaulicht wird, sei für eine anwendungsorientierte Einleitung in die Theorie der hyperelliptischen Kurven auf die Literaturstelle von "A. Menezes, Y.-H. Wu und R. Zuccherato, "An Elementary Introduction to Hyperelliptic Curves", Anhang in Neal Koblitz, "Algebraic aspects of cryptography", Algorithms and Computations in Mathematics, Band 3, Seiten 155 bis 178, Springer.Verlag, 1998 hingewiesen.

Von dieser Literaturstelle weicht die nachstehend verwendete Notation, die sich an der Notation gemäß

- Tanja Lange, "Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/147, 2002, http://eprint.iacr.org/,
- Tanja Lange, "Weighted Coordinates on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/153, 2002, http://eprint.iacr.org/ sowie
- J. Pelzl, T. Wollinger, J. Guajardo, C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves", eingereicht

orientiert:

Wird von zwei hyperelliptischen Kurven C, $\tilde{C}$ vom Geschlecht $g \geq 1$ über dem endlichen Körper K ausgegangen, so lässt sich ein K-Isomorphismus $\phi: C \rightarrow \tilde{C}$ eindeutig zu einem K-Isomorphismus der Jacobischen Varietäten $\phi: J(C) \rightarrow J(\tilde{C})$ erweitern. Anstatt $Q = nD$ in $J(C)$(K) zu berechnen, wobei n eine natürliche Zahl ist und D ein Element von $J(C)$(K) ist, wird

$$Q = \phi^{-1}(n\,\phi(D)) \qquad (1)$$

ausgeführt.

Dies bedeutet mit anderen Worten, dass das schematische Diagramm gemäß Figur 1 kommutativ ist und dass in diesem Diagramm erfindungsgemäß der "längere" Weg über $J(\tilde{C})$(K) gegangen wird (das Bezugszeichen "x n" in Figur 1 bedeutet "Multiplikation mit n").

In diesem Zusammenhang ist die durch diesen K-Isomorphismus der Jacobischen Varietäten implementierte Gegenmaßnahme zum Schutz vor auf der Basis von differentieller Stromanalyse erfolgenden Attacken dann besonders erfolgreich, wenn sich die Darstellungen der Koeffizienten der Kurve C und der Elemente von $J(C)$(K) von den Darstellungen der Bilder unter ϕ stark unterscheiden. Dies kann beispielsweise durch die Multiplikation aller Operanden mit Zufallszahlen erreicht werden.

Nachfolgend wird nicht nur gezeigt, dass dies möglich ist, sondern auch, dass hierzu nur wenige Körperoperationen erforderlich sind.

Eine praktische Realisierung des vorstehend dargelegten Prinzips der Kurvenrandomisierung mittels allgemeiner Isomorphismen von Kurven geht zunächst davon aus, dass

- $g \geq 1$ eine natürliche Zahl ist
- K ein endlicher Körper ist und
- C, $\tilde{C}$ hyperelliptische Kurven des Geschlechts g, die durch Weierstraßsche Gleichungen

$$C : y^2 + h(x)y - f(x) = 0 \quad (2)$$

$$\tilde{C} : y^2 + \tilde{h}(x)y - \tilde{f}(x) = 0 \quad (3)$$

über dem Körper K definiert sind, wobei

- die Polynome f, $\tilde{f}$ normiert vom Grad $2g+1$ in x seien und
- $h(x)$, $\tilde{h}(x)$ höchstens den Grad g haben.

Die hyperelliptische Kurve C besitzt (ebenso wie die hyperelliptische Kurve $\tilde{C}$) keine singulären affinen Punkte, das heißt es gibt keine Paare $(x, y) \varepsilon K \times K$, die gleichzeitig die Gleichung $y^2 + h(x)y - f(x) = 0$ und die partiell abgeleiteten Gleichungen $2y+h(x) = 0$ und $h'(x)y-f'(x) = 0$ erfüllen. Eine äquivalente Bedingung ist, dass die Diskriminante $4f(x) + h(x)^2$ nicht verschwindet (vgl. Theorem 1.7 aus P. Lockhart, "On the discriminant of a hyperelliptic curve", Trans. Amer. Math. Soc. 342 (1994), Nr. 2, Seiten 729 bis 752, MR 94f:11054). Ähnliche Bedingungen gelten für $\tilde{C}$.

Der nichtaffine Punkt der projektiven Komplettierung von C (bzw. von $\tilde{C}$) wird mit "unendlich" bezeichnet. Alle K-Kurvenisomorphismen $\phi: C \rightarrow \tilde{C}$ lassen sich durch Variablentransformationen der Form

$$\phi : (x, y) \mapsto (s^2 x + b, s^{2g+1} y + A(x)) \quad (4)$$

beschreiben (vgl. Proposition 1.2 aus P. Lockhart, "On the discriminant of a hyperelliptic curve", Trans. Amer. Math. Soc. 342 (1994), Nr. 2, Seiten 729 bis 752, MR 94f:11054), für geeignete $s \in K^x$, $b \in K$ und $A(x) \in K[x]$ vom Grad $\leq g$.

Wenn x bzw. y in Gleichung (3) durch $s^{-2}x + b$ bzw. $s^{-(2g+1)}y + A(x)$ ersetzt werden, kann durch Vergleich mit Gleichung (2) geschlossen werden, dass

$$\begin{cases} \tilde{h}(x) = s^{2g+1}\left(\tilde{h}(s^{-2}x+b) + 2A(x)\right) \\ \tilde{f}(x) = s^{2(2g+1)}\left(\tilde{f}(s^{-2}x+b) - A(x)^2 - \tilde{h}(s^{-2}x+b)A(x)\right). \end{cases} \quad (5)$$

Die inverse Transformation ist

$$\begin{cases} \bar{h}(x) = s^{-(2g+1)}\tilde{h}(\hat{x}) - 2A(\hat{x}) \\ \bar{f}(x) = s^{-2(2g+1)}f(\hat{x}) + s^{-(2g+1)}\tilde{h}(\hat{x})A(\hat{x}) - A(\hat{x})^2 \\ \text{wobei } \hat{x} = s^2(x-b). \end{cases} \quad (6)$$

Der Isomorphismus $\phi: C \to \tilde{C}$ induziert einen Isomorphismus von Gruppenvarietäten $\phi: J(C) \to J(\tilde{C})$. Die Jacobische Varietät einer Kurve C ist kanonisch isomorph zur Idealklassengruppe $Cl^0(C)$, die geeigneter für explizite Berechnungen ist; demzufolge ist zu ergründen, wie ϕ als Abbildung $Cl^0(C) \to Cl^0(\tilde{C})$ operiert.

Hierzu ist anzumerken, dass in D. Cantor, "Computing in the jacobian of a hyperelliptic curve", Mathematics of Computation, 48 (1987), Seiten 95 bis 101, Algorithmen für die Rechnungen in der Idealklassengruppe mit der Darstellung in D. Mumford, "Tata Lectures on Theta II", Birkhuser, 1984 entwickelt wurden, die nachfolgend kurz dargestellt werden:

Es sei D der einzige Hauptdivisor vom Grad $\leq g$ in einer gegebenen Divisorklasse auf C, das heißt $D = \Sigma_{P \in S} m_P P - (\Sigma_{P \in S} m_P)_{\text{unendlich}}$,

- wobei die endliche Punktmenge S eine Teilmenge von $C(K)$ ist und als Träger von D bezeichnet wird und
- wobei die Vielfachheiten m_i positive ganze Zahlen mit $\Sigma_{P \in S} m_P \leq g$ sind.

Dann ist die dem Hauptdivisor D zugehörige Idealklasse durch ein Paar eindeutig bestimmter Polynome $U(t)$, $V(t) \in K[t]$ mit den folgenden Eigenschaften gegeben: $g \geq \deg_t U \geq \deg_t V$, U ist normiert und

$$\begin{cases} U(t) = \prod_{P \in S} (t - x_P)^{m_P} \\ V(x_P) = y_P \text{ für alle } P \in S \\ U(t) \text{ teilt } V(t)^2 + V(t)h(t) - f(t) \end{cases} \quad (7)$$

Gemäß der folgenden Nomenklatur soll $[U(t), V(t)]$ den reduzierten Divisor D darstellen.

Ziel ist es, zwei Polynome $\tilde{U}(t), \tilde{V}(t) \in K[t]$ zu finden, die ähnliche Eigenschaften wie $U(t)$, $V(t)$ aufweisen, jedoch zum Divisor $\phi(D) = \Sigma_{P \in S} m_P \phi(P) - (\Sigma_{P \in S} m_P)_{\text{unendlich}}$ auf C anstatt D gehören. Dies bedeutet mit anderen Worten, dass sich für alle Körpererweiterungen L/K die folgenden Beziehungen ergeben sollen:

$$\begin{array}{ccccc} D = \sum_{P \in S} m_P P - \left(\sum_{P \in S} m_P\right)\infty & \xrightarrow{\phi} & \sum_{P \in S} m_P \phi(P) - \left(\sum_{P \in S} m_P\right)\infty = \phi(D) \\ \| & & \| \\ [U(t), V(t)] & \xrightarrow{\phi} & [\tilde{U}(t), \tilde{V}(t)] \end{array}$$

Es ist klar, wie die gesuchten Polynome zu konstruieren sind. Offensichtlich ist

$$\begin{aligned} \tilde{U}(t) &= \prod_{P \in S} (t - x_{\phi(P)})^{m_P} = \prod_{P \in S} (t - s^{-2} x_P - b)^{m_P} \\ &= s^{-2 \sum_{P \in S} m_P} U(s^2(t-b)) = s^{-2 \deg_t U} U(s^2(t-b)) \end{aligned} \quad (8)$$

Ferner ist $\tilde{V}(x_{\phi(P)}) = y_{\phi(P)}$ für alle P ε S, das heißt

$$\tilde{V}(s^{-2} x_P + b) = s^{-(2g+1)} y_P + A(x_P) = s^{-(2g+1)} V(x_P) + A(x_P)$$

Ein geeigneter Kandidat ist

$$\tilde{V}(t) = s^{-(2g+1)} V(s^2(t-b)) + A(s^2(t-b)) \quad (9)$$

In der Tat geben die Gleichung (8) und die Gleichung (9) die richtige Antwort; dies folgt aus der Eindeutigkeit der Darstellung eines reduzierten Divisors: $\tilde{U}(t)$ und $\tilde{V}(t)$ sind über K definiert, $\deg\tilde{V} = \deg V < \deg U = \deg\tilde{U}$ und die Feststellung, dass $\tilde{U}(t)$ tatsächlich $\tilde{V}(t)^2 + \tilde{V}(t)\tilde{h}(t) - \tilde{f}(t)$ teilt, ist leicht.

Nachstehend wird nun der Fall betrachtet, dass K ein Körper von ungerader Charakteristik ist. Es wird angenommen, dass $h(x) = \tilde{h}(x) = 0$ ist, denn die definierenden Gleichungen können bei der Variablentransformation gemäß $y \to y - h(x)/2$ und $y \to y - \tilde{h}(x)/2$ immer in diese Form gebracht werden. Der Vorteil besteht darin, dass der Cantorsche Algorithmus viel schneller läuft, und aus demselben Grund wurden explizite Formeln in ungerader Charakteristik unter obiger Annahme entwickelt. Die Gleichungen für C, $\tilde{C}$ sind

$$C : y^2 - f(x) = 0 \tag{10}$$

$$\tilde{C} : y^2 - \tilde{f}(x) = 0. \tag{11}$$

Dies beinhaltet bei Gleichung (6), dass $A(x) = 0$ ist.

Falls char K $\nmid 2g+1$ ist, kann darüber hinaus davon ausgegangen werden, dass der zur zweithöchsten Potenz von x in $f(x)$ gehörende Koeffizient f_{2g} (und der in $\tilde{f}(x)$) verschwindet, denn es kann stets eine Variablentransformation gemäß $x \to x - f_{2g}/(2g+1)$ durchgeführt werden. In diesem Fall muss kraft Gleichung (6) $b = 0$ sein.

Also ist ϕ vom Typ

$$\phi : (x, y) \mapsto (s^{-2}x, s^{-(2g+1)}y)$$

mit $s \in K^x$. Es sollen hinsichtlich der ungeraden Charakteristik nur Isomorphismen dieses Typs betrachtet werden, auch falls char K = 2g+1. Die Formel zu $\tilde{f}$ ist dann

$$\tilde{f}(x) = s^{-2(2g+1)} f(s^2 x).$$

Diese Randomisierung ändert alle Koeffizienten der Weierstraßschen Gleichung und der zwei den reduzierten Divisor darstellenden Polynome (ausgeschlossen die an 1 festverdrahtet), und zwar

$$\bar{U}(t) = s^{-2\deg_t U} U(s^2 t), \quad \bar{V}(t) = s^{-(2g+1)} V(s^2 t)$$

Folglich kann diese Randomisierung als eine sichere Gegenmaßnahme zum Abwehren von auf differentieller Stromanalyse beruhenden Angriffen auf Implementierungen hyperelliptischer Kryptosysteme bei einem Körper K von ungerader Charakteristik erachtet werden.

In einer expliziten Beschreibung dieser mittels eines implementatorischen Tricks realisierten, sehr schnellen Kurvenrandomisierung bei einem Körper K von ungerader Charakteristik wird zunächst ein Zufallselement $s \in K^x$ ausgewählt und sodann seine multiplikative Inverse berechnet. Der Grund dafür ist, dass s^{-1} für ϕ und s für ϕ^{-1} benötigt werden.

Nachstehend wird nun ϕ im Detail beschrieben. Aus

$$f(x) = x^{2g+1} + \sum_{i=0}^{2g-1} f_i x^i$$

ist erhaltbar

$$\bar{f}(x) = x^{2g+1} + \sum_{i=0}^{2g-1} s^{2i-2(2g+1)} f_i x^i$$

Für allgemeine $U(t)$ und $V(t)$ ist

$$U(t) = t^g + \sum_{i=0}^{g-1} U_i t^i \quad \text{und} \quad V(t) = \sum_{i=0}^{g-1} V_i t^i,$$

so dass

$$\bar{U}(t) = t^g + \sum_{i=0}^{g-1} s^{2i-2g} U_i t^i \quad \text{und} \quad \bar{V}(t) = \sum_{i=0}^{g-1} s^{2i-(2g+1)} V_i t^i$$

Um ϕ auf der Kurve und auf einen Basisdivisor $[U(t), V(t)]$ anzuwenden, wird s^{-k} für $k = 2, 3, ..., 2g+1$ nacheinander berechnet:

- wenn k gerade ist, wird $U_{g-k/2}$ und (wenn k ungleich 2) $f_{2g+1-k/2}$ mit s^{-k} multipliziert,
- wenn k ungerade ist, wird $V_{g-(k-1)/2}$ mit s^{-k} multipliziert.

Für $k = 2g+2, 2g+4, ..., 2(2g+1)$ wird s^{-k} durch wiederholte Multiplikationen mit s^{-2} berechnet und $f_{2g+1-k/2}$ mit s^{-k} multipliziert. Zusammen sind dies $7g+1$ Multiplikationen; ϕ^{-1} benötigt nur $4g$ Multiplikationen in K.

Falls die Kurve oder zumindest der Grundkörper festgelegt ist, gibt es auch einen implementatorischen Trick, der eingesetzt werden kann, um die Berechnung der Inversion s^{-1} des Elements s bei jedem Gebrauch des kryptographischen Geräts zu vermeiden.

Von vornherein werden während der Initialisierungsphase des kryptographischen Geräts zufällig ein Paar von Körperelementen (s_0, s_0^{-1}) zusammen mit mehreren weiteren derartigen Paaren $(\kappa_i, \kappa_i^{-1})$ erzeugt und im E^2PROM gespeichert.

Dann wird vor jeder kryptographischen Operation zufällig ein Index i gewählt; damit wird (s_0, s_0^{-1}) im E^2PROM durch $(\kappa_i s_0, \kappa_i^{-1} \cdot s_0^{-1})$ ersetzt. Das letztere Paar wird dann anstatt (s, s^{-1}) für die Kurvenrandomisierung im gegenwärtigen Lauf des kryptographischen Geräts eingesetzt.

Zusammenfassend lässt sich mithin feststellen, dass die Kurvenrandomisierung in ungerader Charakteristik eine effektive und effiziente Schutzmaßnahme gegen auf die Methode der differentiellen Stromanalyse gestützte Angriffe ist. Die Gesamtanzahl notwendiger Körperoperationen in K ist $11g+1$.

In der Praxis ist dies mit der Anzahl von Körperoperationen, für einzelne Gruppenoperationen vergleichbar und oft viel weniger, als die Formeln in

- Tanja Lange, "Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/147, 2002, http://eprint.iacr.org/,
- Tanja Lange, "Weighted Coordinates on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/153, 2002, http://eprint.iacr.org/ sowie
- J. Pelzl, T. Wollinger, J. Guajardo, C. Paar, "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves", eingereicht

zeigen.

Die vorstehend hinsichtlich der allgemeinen Isomorphismen von Kurven aufgeführten Argumente gelten in unveränderter Weise auch für den nachstehend diskutierten Fall, dass K ein Körper von gerader Charakteristik ist. In diesem Falle muss jedoch $h(x)\bar{h}(x)$ ungleich Null sein; dies bedeutet mit anderen Worten, dass die Anwendung allgemeiner Isomorphismen weniger effizient als im Falle der ungeraden Charakteristik ist.

Anstelle der allgemeinen Isomorphismen gemäß Gleichung (4) wird $b = 0$ und $A(x) = 0$ angenommen und wie im Falle der ungeraden Charakteristik gearbeitet. Die Isomorphismen der Form

$$\phi : (x, y) \mapsto \left(s^{-2}x,\ s^{-(2g+1)}y\right) \tag{12}$$

für allgemeine $s \in F_{2^d} \setminus F_2$ randomisieren alle Koeffizienten der Gleichung wie folgt:

$$\begin{cases} \bar{h}(x) = s^{-(2g+1)}h(s^2x) \\ \bar{f}(x) = s^{-2(2g+1)}f(s^2x) \end{cases} \tag{13}$$

Wie bei der vorstehenden expliziten Beschreibung der mittels eines implementatorischen Tricks realisierten, sehr schnellen Kurvenrandomisierung bei einem Körper K von ungerader Charakteristik wird auch bei einer expliziten Beschreibung der mittels eines implementatorischen Tricks realisierten, sehr schnellen Kurvenrandomisierung bei einem Körper K von gerader Charakteristik aus

$$f(x) = x^{2g+1} + \sum_{i=0}^{2g-1} f_i x^i \quad \text{und} \quad h(x) = \sum_{i=0}^{g} h_i x^i,$$

dann

$$\tilde{f}(x) = x^{2g+1} + \sum_{i=0}^{2g-1} s^{2i-2(2g+1)} f_i x^i \quad \text{und} \quad \tilde{h}(x) = \sum_{i=0}^{g} s^{2i-(2g+1)} h_i x^i$$

und die Formeln für $\tilde{U}$, $\tilde{V}$ lauten wiederum

$$\tilde{U}(t) = t^g + \sum_{i=0}^{g-1} s^{2i-2g} U_i t^i \quad \text{und} \quad \tilde{V}(t) = \sum_{i=0}^{g-1} s^{2i-(2g+1)} V_i t^i$$

Die Folgerung ist, dass keine allgemeinen Isomorphismen vom Typ gemäß Gleichung (4) benötigt werden, sondern dass diejenigen vom Typ gemäß Gleichung (12) ausreichen, um alle Bits der internen Darstellungen effizient zu randomisieren.

Die Koeffizienten von $\tilde{h}(x)$ werden aus den Koeffizienten von $h(x)$ ähnlich wie die Koeffizienten von $\tilde{V}(t)$ berechnet: Für $k = 3, 5, \ldots, 2g+1$ werden $V_{g-(k-1)/2}$ und $h_{g-(k-1)/2}$ mit s^{-k} multipliziert; außerdem wird h_g mit s^{-1} multipliziert; dies bedeutet, dass höchstens $g+1$ Körperoperationen mehr als im Falle ungerader Charakteristik erforderlich sind, und die sämtlichen Kosten für die Anwendung von ϕ sind $8g+2$ Multiplikationen, nachdem s gewählt und s^{-1} berechnet ist. Der vorstehend beschriebene implementatorische Trick ist hier nicht notwendig, denn die Inversion in binären Körpern ist ausreichend schnell.

Nachstehend wird nun eine Fallunterscheidung für konstantes h und für nichtkonstantes, jedoch über F_2 definiertes h untersucht werden:

In gerader Charakteristik ist darauf zu achten, welche Probleme entstehen, falls die Koeffizienten der definierenden Gleichungen aus Durchsatzgründen beschränkt werden, wobei der einfachste Fall betrachtet werden soll, dass $h(x)$ eine nichtverschwindende Konstante ist, denn bei Gleichung (6) ist $\tilde{h}(x)$ ebenfalls konstant und nichtverschwindend.

Nun ist es aber ein bekanntes Resultat der algebraischen Geometrie, dass Kurven mit der Gleichung $y^2 + cy = f(x)$ mit nichtverschwindendem c und mit $\deg f = 5$ supersingulär (vgl. Theorem 9 in S. D. Galbraith, "Supersingular curves in cryptography", in C. Boyd (Hrsg.), ASIACRYPT 2001, "Lecture Notes in Computer Science", Band 2248, Seiten 495 bis 513, Springer-Verlag, 2001), also nicht geeignet für die hier interessierenden kryptographischen Anwendungen sind.

Demgegenüber ist keine hyperelliptische Kurve des Geschlechts $g = 3$ in gerader Charakteristik supersingulär (vgl. J. Scholten und H. J. Zhu, "Hyperelliptic curves in characteristic 2", Inter. Math. Research Notices, 17 (2002), Seiten 905 bis 917), also kann im Prinzip von Kurven mit der Gleichung $y^2 + cy = f(x)$ mit nichtverschwindendem c und mit $\deg f = 7$ unter der Voraussetzung Gebrauch gemacht werden, dass Erweiterungsgrad und Gruppenordnung angemessen ausgewählt werden.

Obwohl in der von J. Pelzl, T. Wollinger, J. Guajardo und C. Paar eingereichten Arbeit "Hyperelliptic Curve Cryptosystems: Closing the Performance Gap to Elliptic Curves" eine sehr schnelle Verdopplungsformel nur für den Fall $h(x) = 1$ gegeben wird, kann die Geschwindigkeit der Divisorenverdopplung auch dann beträchtlich beschleunigt werden, wenn $h(x)$ eine nichtverschwindende Konstante ist. Es ist $\tilde{h}(x) = s^{-(2g+1)}c = s^{-7}c$; dies macht den Fall von Kurven des Geschlechts $g = 2$ wichtig.

Im Falle eines nichtkonstanten h werden die Koeffizienten von $h(x)$ aus Gründen der Geschwindigkeit oft in F_2 gewählt (vgl. zum Beispiel Tanja Lange, "Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/147, 2002, http://eprint.iacr.org/ oder Tanja Lange, "Weighted Coordinates on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/153, 2002, http://eprint.iacr.org/).

In diesem Falle eines nichtkonstanten, jedoch über F_2 definierten h liegt aufgrund der Gleichung (6) eine Äquivalenz mit folgender Frage vor: Wenn $h(x) \in F_2[x]$, für welche $b \in K$ und für welche $s \in K^x$ ist $\tilde{h}(x) = s^{-(2g+1)}h(s^2(x-b)) \in F_2[x]$?

Falls $r = (2g+1) - 2 \deg h$ ist, ist der führende Koeffizient s^{-r} von $\tilde{h}(x)$ gleich Eins, denn dieser führende Koeffizient verschwindet nicht; die Zahl r ist ungerade, positiv und $\leq 2g-1$.

Das Kryptosystem muss dem Index-Calculus-Angriff von Gaudry (vgl. P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves", in "Advances in Cryptology - Eurocrypt 2000", Seiten 19 bis 34, "Lecture Notes" in Computer Science, Band 1807, Springer-Verlag, Berlin, Heidelberg, 2000) widerstehen, also ist $g \leq 4$; folglich ist $r \leq 7$, und für r gibt es nur sehr wenige mögliche Werte; dies macht ihrer Randomisierung unnötig.

Es sei der Erweiterungsgrad $d = [K : F_2]$.

In diesem Zusammenhang ist anzumerken, dass für einen Schutz vor Angriffen durch Weil-Abstieg (vgl. G. Frey, "How to disguise an elliptic curve (Weil descent)", Talk at ECC '98, Waterloo, 1998 (Folien verfügbar unter http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html); G. Frey, "Applications of arithmetical geometry to cryptographic constructions", in "Finite fields and applications (Augsburg, 1999), Seiten 128 bis 161, Springer, Berlin, 2001) für den Erweiterungsgrad d entweder eine Primzahl p in der Größenordnung von $\geq 160/g$ oder zweimal eine Primzahl p in der Größenordnung von $\geq 80/g$ gewählt wird.

Die möglichen Werte von s sind Nullstellen von irreduziblen Faktoren von, X^r-1, deren Grad d teilt. Falls $d = p \geq 160/g \geq 40$ (= bevorzugter Fall), ist $s = 1$; Falls $d = 2p$ mit $p \geq 80/g \geq 20$, kann s nur eine Nullstelle eines Faktors über F_2 von X^r-1 vom Grad 1 oder 2 sein. Eine schnelle Auflistung solcher Faktoren (zu beachten ist, dass r ungerade und ≤ 7) zeigt, dass entweder $s = 1$ oder $r = 3$ und $s^2 + s + 1 = 0$. Wenn zwei Koeffizienten von $h(x)$ nicht verschwinden, dann ist stets $s = 1$.

Wird nun von σ: $\alpha \rightarrow \alpha^2$ als Frobenius-Automorphismus von K/F_2 ausgegangen, ist $h(-b^{\sigma}) = h(-b)^{\sigma} = h(-b) \varepsilon F_2$ für alle j, weil $\tilde{h}(x) = h(x-b) \varepsilon F_2[x]$. Dies bedeutet mit anderen Worten, dass alle Konjugierten von $-b$ unter dem Frobenius Lösungen von $h(x)-h(-b) = 0$ sind. Falls b kein Element von F_2 ist, gibt es mindestens $p \geq 80/g$ solcher Konjugierten, wobei der Grad von $h(x)$ höchstens $g \leq 4$ ist. Aus diesem Grunde muss b Element von F_2 sein: Es gibt nur zwei Möglichkeiten für b, also ist eine Randomisierung von b auch nicht sehr sinnvoll.

Es kann also schlussfolgert werden, dass die relevanten Isomorphismen vom Typ

$$\phi : (x, y) \rightarrow (x, y + A(x))$$

sind, wobei $A(x) \varepsilon K[x]$ vom Grad $\leq g$ ist.

Im Sinne eines hyperelliptischen Analogons ist die Situation hier also der in der vorstehend zitierten Arbeit von M. Joye und von C. Tymen beschriebenen Situation bei der Randomisierung von elliptischen Kurven ähnlich, denn es kann nur eines der beiden Polynome oder nur eine Hälfte der Koordinaten leistungsfähig randomisiert werden.

Tatsächlich ist die Situation sogar schlechter, denn infolge Gleichung (6) werden nicht alle Koeffizienten von f in $\tilde{f}$ randomisiert, was die Wahrscheinlichkeit eines auf differentielle Stromanalyse (= D[ifferential]P[ower]A[nalysis]) gestützten erfolgreichen Angriffs erhöht, wenn die Kurvenrandomisierung allein eingesetzt wird.

Zusammenfassend lässt sich zur vorstehend diskutierten Methode der Kurvenrandomisierung mithin feststellen, dass diese Gegenmaßnahme für hyperelliptische Kurven des Geschlechts 2 in gerader Charakteristik

- entweder nicht ausreichend ist, weil zu wenige Koeffizienten randomisiert werden können,
- oder die Leistung des kryptographischen Systems hemmt, indem die Gegenmaßnahme die allgemeinen Isomorphismen gemäß Gleichung (4) verwendet und die Koeffizienten von h außerhalb F^2 liegen lässt.

Im Falle von Geschlecht 3 können Kurven Gleichung $y^2 + cy = f(x)$ und allgemeine Isomorphismen eingesetzt werden. In diesem Falle genügt es, in Gleichung (4) $b = 0$ und $A(x) = 0$ zu fixieren, und wie am Ende der vorstehenden Beschreibung zum Falle der ungeraden Charakteristik fortzufahren, um alle Koeffizienten in vernünftiger Weise zu randomisieren.

In allen weiteren Fällen empfehlen sich andere Techniken, wie etwa die Divisorenrandomisierung, die auch in ungerader Charakteristik arbeitet und die nachfolgend als zweites Ausführungsbeispiel dargelegt wird, das

- in Kombination mit dem ersten Ausführungsbeispiel der Kurvenrandomisierung oder
- unabhängig vom ersten Ausführungsbeispiel der Kurvenrandomisierung

ausführbar ist.

Bei der Technik der Divisorenrandomisierung werden die Bits der Darstellung eines reduzierten Divisors, der üblicherweise das Basiselement des Kryptosystems ist, oder ein Zwischenergebnis der Skalarmultiplikation geändert. Die Technik der Divisorenrandomisierung wird eingesetzt, wenn ein Gruppenelement auf mehrere unterschiedliche Weisen dargestellt werden kann.

Hervorhebenswerte Beispiele aus dem Stand der Technik sind die projektiven Koordinaten auf elliptischen Kurven: Zwei Tripel (X, Y, Z) und (X', Y', Z') stellen den gleichen Punkt dar, wenn ein nichtverschwindendes Element s im Grundkörper existiert derart, dass $X = sX'$, $Y = sY'$ und $Z = sZ'$. In Jacobischen Koordinaten (vgl. D. V. Chudnovsky und G. V. Chudnovsky, "Sequences of numbers generated by addition in formal groups and new primality and factoring tests", Advances in Applied Mathematics, 7 (1987), Seiten 385 bis 434) stellen zwei Tripel (X, Y, Z) und (X', Y', Z') den gleichen Punkt dar, wenn $X = s^2X'$, $Y = s^3Y'$ und $Z = sZ'$ mit $s \in K^x$ ist.

Vor kurzem sind alternative Koordinatensysteme für hyperelliptische Kurven des Geschlechts 2 vorgeschlagen worden. Ein inversionsfreies System durch Miyamoto et al (vgl. Y. Miyamoto, H. Doi, K. Matsuo, J. Chao und S. Tsuji, "A fast addition algorithm of genus two hyperelliptic curve", in Proceedings of SCIS 2002, IEICE Japan, Seiten 497 bis 502, 2002, auf japanisch), das auf der hyperelliptischen Entsprechung der projektiven Koordinaten für elliptische Kurven operiert, wurde ausgedehnt und verbessert durch Lange (vgl. Tanja Lange, "Inversion-Free Arithmetic on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/147, 2002, http://eprint.iacr.org/), die auch eine Entsprechung der Jacobischen Koordinaten entwickelte, nämlich die sogenannten gewichteten Koordinaten (vgl. Tanja Lange, "Weighted Coordinates on Genus 2 Hyperelliptic Curves", Cryptology ePrint Archive, Report 2002/153, 2002, http://eprint.iacr.org/). Bei Geschlecht 3 sind keine ähnlichen Systeme bekannt.

Je größer das Geschlecht der Kurve ist, desto kleiner wird bei gleicher Gruppenordnung der Grundkörper, und damit wird das Geschwindigkeitsverhältnis von Inversionen zu Multiplikationen kleiner. Dies macht inversionsfreie Formeln für Geschlecht 3 weniger attraktiv, denn es würde eine Inversion gegen viele Multiplikationen eingetauscht. Andererseits existieren bereits effiziente Bitrandomisierungsverfahren für Kurven des Geschlechts 3 sowohl für Fälle ungerader Charakteristik als auch für Fälle gerader Charakteristik.

In projektiven Koordinaten (Geschlecht 2) wird ein Divisor D mit zugehörigem Polynompaar als ein Quintupel $[U_1, U_0, V_1, V_0, Z]$ dargestellt, wobei
$U(t) = t^2 + U_1 t/Z + U_0/Z$ und $V(t) = V_1 t/Z + V_0/Z$.

Die Divisorenrandomisierung arbeitet wie folgt: Ein zufälliges $s \in K^x$ wird gewählt, und die folgende Umwandlung wird angewendet:
$[U_1, U_0, V_1, V_0, Z] \rightarrow [sU_1, sU_0, sV_1, sV_0, sZ]$.

In gewichteten Koordinaten wird ein Divisor D durch ein Sextupel $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ dargestellt, wobei
$U(t) = t^2 + U_1 t/Z_1^2 + U_0/Z_1^2$ und $V(t) = V_1 t/(Z_1^3 Z_2) + V_0/(Z_1^3 Z_2)$.

Um den Basisdivisor oder eine Zwischenberechnung unsichtbar zu machen, werden zwei Elemente s_1, s_2 in K^x zufällig ausgewählt und die folgende Transformation wird durchgeführt:
$[U_1, U_0, V_1, V_0, Z_1, Z_2] \rightarrow [s_1^2 U_1, s_1^2 U_0, s_1^3 s_2 V_1, s_1^3 s_2 V_0, s_1 Z_1, s_2 Z_2]$

Wenn die zusätzlichen optionalen Koordinaten
$z_1 = Z_1^2$, $z_2 = Z_2^2$, $z_3 = Z_1 Z_2$ und $z_4 = z_1 z_2 = z_3^2$
verwendet werden, sind diese zusätzlichen optionalen Koordinaten auch zu aktualisieren; die schnellste Weise der Aktualisierung besteht darin, sie von den Bildern von Z_1 und Z_2 durch drei Quadrierungen und eine Multiplikation zurückzugewinnen.

Die beiden erfindungsgemäß vorgeschlagenen Maßnahmen, nämlich die Maßnahme der Kurvenrandomisierung (= erstes Ausführungsbeispiel) und die Maßnahme der Divisorenrandomisierung (= zweites Ausführungsbeispiel) stärken jeweils für sich genommen wie auch in Kombination miteinander hyperelliptische Kryptosysteme gegen differentielle Stromanalyse. Sowohl die Technik der Kurvenrandomisierung als auch die Technik der Divisorenrandomisierung ist einfach einzuführen und wirken sich auf den Durchsatz in lediglich unerheblicher Weise aus.

Das Verfahren gemäß dem ersten Ausführungsbeispiel, das heißt die Kurvenrandomisierung transportiert die Skalarmultiplikation in der Jacobischen Varietät in eine zufällig gewählte isomorphe Gruppe. Die Skalarmultiplikation wird in dieser zweiten Gruppe durchgeführt, und das Ergebnis der Skalarmultiplikation wird wieder in die erste Gruppe zurückgebracht. Die Methode der Kurvenrandomisierung kann auf Kurven beliebigen Geschlechts angewendet werden.

Das Verfahren gemäß dem zweiten Ausführungsbeispiel, das heißt die Divisorenrandomisierung ist eine hyperelliptische Variante von Corons dritter Gegenmaßnahme. Die Divisorenrandomisierung ist nur bei Kurvenfamilien anwendbar, von denen Koordinatensysteme für die Gruppenoperationen in den zugehörigen Jacobischen Varietäten bekannt sind, die den elliptischen projektiven oder Jacobischen entsprechen.

Die beiden vorstehend beschriebenen Gegenmaßnahmen zum Abwehren von auf differentieller Stromanalyse beruhenden Angriffen auf Implementierungen hyperelliptischer Kryptosysteme können unabhängig voneinander oder gleichzeitig miteinander eingesetzt werden.

BEZUGSZEICHENLISTE

C	hyperelliptische Kurve
$\tilde{C}$	transformierte hyperelliptische Kurve
D	Divisor, insbesondere reduzierter Divisor
g	Geschlecht
J	Jacobische Varietät
K	Körper, insbesondere endlicher Körper
n	Skalar
s	Element, insbesondere nichtverschwindendes Element
s_1	erstes Element, insbesondere nichtverschwindendes erstes Element
s_2	zweites Element, insbesondere nichtverschwindendes zweites Element
t	Variable
ϕ	Abbildung
ϕ^{-1}	inverse Abbildung
$[U_1, U_0, V_1, V_0, Z]$	Quintupel
$[sU_1, sU_0, sV_1, sV_0, sZ]$	umgewandeltes Quintupel
$[U_1, U_0, V_1, V_0, Z_1, Z_2]$	Sextupel
$[s_1^2U_1, s_1^2U_0, s_1^3s_2V_1, s_1^3s_2V_0, s_1Z_1, s_2Z_2]$	umgewandeltes Sextupel

PATENTANSPRÜCHE

1. Verfahren zum Abwehren mindestens eines Angriffs, das mittels differentieller Stromanalyse bei mindestens einem hyperelliptischen Kryptosystem, insbesondere bei mindestens einem hyperelliptischen Public-Key-Kryptosystem, erfolgt, das durch mindestens eine hyperelliptische Kurve (C) beliebigen Geschlechts (g) über einem endlichen Körper (K) in einer ersten Gruppe gegeben ist, wobei die hyperelliptische Kurve (C) durch mindestens einen Koeffizienten gegeben ist,
dadurch gekennzeichnet,
dass die hyperelliptische Kurve (C) und/oder mindestens ein Element der ersten Gruppe, insbesondere mindestens ein insbesondere reduzierter Divisor und/oder mindestens ein Zwischenergebnis einer Skalarmultiplikation, randomisiert wird.

2. Verfahren gemäß Anspruch 1,
dadurch gekennzeichnet,
dass die im Rahmen des hyperelliptischen Kryptosystems zu verarbeitenden und/oder zu verschlüsselnden Bits von den Operanden durch die hyperelliptische Kurve (C), insbesondere durch mindestens einen Koeffizienten der hyperelliptischen Kurve (C), und/oder durch mindestens ein Basiselement des Kryptosystems, wie etwa durch mindestens einen insbesondere reduzierten Divisor und/oder durch mindestens ein Zwischenergebnis einer Skalarmultiplikation, repräsentiert werden.

3. Verfahren gemäß Anspruch 1 oder 2,
dadurch gekennzeichnet,
dass mindestens eine Skalarmultiplikation in der Jacobischen Varietät $J(C)(\mathrm{K})$ der hyperelliptischen Kurve (C) in einer von der ersten Gruppe verschiedenen sowie zur ersten Gruppe isomorphen, insbesondere zufällig gewählten zweiten Gruppe erfolgt.

4. Verfahren gemäß Anspruch 3,
gekennzeichnet durch
die folgenden Schritte:

- Transformieren der Jacobischen Varietät $J(C)(\mathrm{K})$ der hyperelliptischen Kurve (C) mittels mindestens einer Abbildung (ϕ), insbesondere mittels mindestens eines K-Isomorphismus, in die Jacobische Varietät $J(\tilde{C})(\mathrm{K})$ der transformierten hyperelliptischen Kurve $(\tilde{C} = \phi(C))$;
- Multiplizieren der Jacobischen Varietät $J(\tilde{C})(\mathrm{K})$ der transformierten hyperelliptischen Kurve $(\tilde{C})$ mit mindestens einem Skalar (n); und
- Rücktransformieren der mit dem Skalar (n) multiplizierten Jacobischen Varietät $J(\tilde{C})(\mathrm{K})$ der transformierten hyperelliptischen Kurve $(\tilde{C})$ mittels der zur Abbildung (ϕ) inversen Abbildung (ϕ^{-1}) in eine mit dem Skalar (n) multiplizierte Jacobischen Varietät $J(C)$ der hyperelliptischen Kurve (C),
- wobei
  -- die Abbildung (ϕ) dem Übergang von der ersten Gruppe in die zweite Gruppe und
  -- die inverse Abbildung (ϕ^{-1}) dem Übergang von der zweiten Gruppe in die erste Gruppe

entspricht.

5. Verfahren gemäß mindestens einem der Ansprüche 1 bis 4,
gekennzeichnet durch
die folgenden Schritte:

- Darstellen mindestens eines insbesondere reduzierten Divisors (D) mit zugehörigem Polynompaar als mindestens ein Quintupel $[U_1, U_0, V_1, V_0, Z]$ in projektiven Koordinaten,
  wobei $U(t) = t^2 + U_1 t/Z + U_0/Z$ und $V(t) = V_1 t/Z + V_0/Z$;
- Auswählen, insbesondere zufälliges Auswählen, mindestens eines nichtverschwindenden Elements (s) aus dem Körper (K^x); und
- Umwandeln des Quintupels $[U_1, U_0, V_1, V_0, Z]$ mittels des ausgewählten Elements (s) in das umgewandelte Quintupel $[sU_1, sU_0, sV_1, sV_0, sZ]$.

6. Verfahren gemäß mindestens einem der Ansprüche 1 bis 4,
gekennzeichnet durch
die folgenden Schritte:

- Darstellen mindestens eines insbesondere reduzierten Divisors (D) mit zugehörigem Polynompaar als mindestens ein Sextupel $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ in projektiven Koordinaten,
  wobei $U(t) = t^2 + U_1 t/Z_1^2 + U_0/Z_1^2$ und $V(t) = V_1 t/(Z_1^3 Z_2) + V_0/(Z_1^3 Z_2)$;
- Auswählen, insbesondere zufälliges Auswählen, mindestens zweier jeweils nichtverschwindender Elemente (s_1, s_2) aus dem Körper (K^x); und
- Umwandeln des Sextupels $[U_1, U_0, V_1, V_0, Z_1, Z_2]$ mittels der ausgewählten Elemente (s_1, s_2) in das umgewandelte Sextupel $[s_1^2 U_1, s_1^2 U_0, s_1^3 s_2 V_1, s_1^3 s_2 V_0, s_1 Z_1, s_2 Z_2]$.

7. Verfahren gemäß mindestens einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass das Verfahren auf mindestens einem insbesondere mindestens einer Chipkarte und/oder insbesondere mindestens einer Smart-Card zugeordneten Mikroprozessor implementiert wird.

8. Mikroprozessor, arbeitend gemäß einem Verfahren gemäß mindestens einem der Ansprüche 1 bis 7.

9. Vorrichtung, insbesondere Chipkarte und/oder insbesondere Smart-Card, aufweisend mindestens einen Mikroprozessor gemäß Anspruch 8.

10. Verwendung eines Verfahrens gemäß mindestens einem der Ansprüche 1 bis 7 und/oder mindestens eines Mikroprozessors gemäß Anspruch 8 und/oder mindestens einer Vorrichtung, insbesondere mindestens einer Chipkarte und/oder insbesondere mindestens einer Smart-Card, gemäß Anspruch 9 beim Abwehren mindestens eines mittels differentieller Stromanalyse auf mindestens ein hyperelliptisches Kryptosystem, insbesondere auf mindestens ein hyperelliptisches Public-Key-Kryptosystem, erfolgenden Angriffs.

ZUSAMMENFASSUNG

Verfahren zum Abwehren von mittels differentieller Stromanalyse erfolgenden Angriffen

Um ein Verfahren zum Abwehren mindestens eines Angriffs, das mittels differentieller Stromanalyse bei mindestens einem hyperelliptischen Kryptosystem, insbesondere bei mindestens einem hyperelliptischen Public-Key-Kryptosystem, erfolgt, das durch mindestens eine hyperelliptische Kurve (C) beliebigen Geschlechts (g) über einem endlichen Körper (K) in einer ersten Gruppe gegeben ist, wobei die hyperelliptische Kurve (C) durch mindestens einen Koeffizienten gegeben ist, so weiterzubilden, dass ein wesentlicher Beitrag zu einer effizienten und sicheren Implementierung des hyperelliptischen Kryptosystems geleistet werden kann, wird vorgeschlagen, dass die hyperelliptische Kurve (C) und/oder mindestens ein Element der ersten Gruppe, insbesondere mindestens ein insbesondere reduzierter Divisor und/oder mindestens ein Zwischenergebnis einer Skalarmultiplikation, randomisiert wird.

Fig. 1

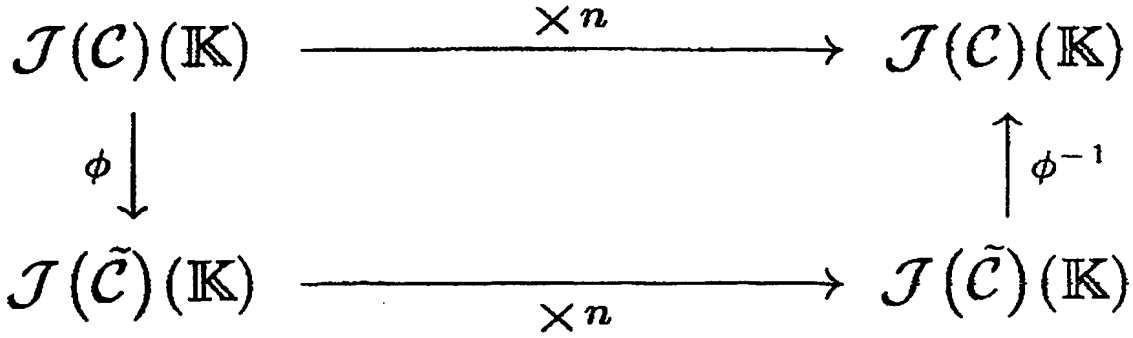
$\mathcal{J}(\mathcal{C})(\mathbb{K})$
$\times n$
$\mathcal{J}(\mathcal{C})(\mathbb{K})$
ϕ
ϕ^{-1}
$\mathcal{J}(\tilde{\mathcal{C}})(\mathbb{K})$
$\times n$
$\mathcal{J}(\tilde{\mathcal{C}})(\mathbb{K})$

Fig. 1

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.